DETAILED ACTION

1. This communication is responsive to Amendment, filed 12/10/2007.

Claims 1-34 are pending in this application. Claims 1, 13, 25, 34 are independent claims. Claims 1, 13, 25 have been amended. This action is made Final.

Information Disclosure Statement

2. The information disclosure statements (IDSs) submitted on 02/08/08, 01/25/08, 01/09/08 are in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statements are being considered by the examiner.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless:
>
> (e) the invention was described in
>
> (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or
>
> (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claim 34 is rejected under 35 U.S.C. 102(e) as being anticipated by Spilo et al. (US Patent No. 6,208,999).

Spilo anticipated independent claim 34 by the following:

As per claim 34, Spilo teaches a serverless backup method comprising:

opening a file system root directory *(i.e. The file system of the invention includes file identification information with file data, thereby enhancing prospects for file recovery in the event of file system damage. Moreover, the entire directory structure for the storage device, including all subdirectories, is maintained in a single data structure. If this data structure is damaged, it can be completely recreated from information recovered from other areas of the storage device, col. 4, lines 38-46)*;

parsing the file system root directory for allocation tables of each file and finding attributes of each file *(Each directory entry within the directory structure contains the entire pathname to a data file. Accordingly, a hierarchical structure, such as a FAT system, is simulated by the invention. In a preferred embodiment, the invention is compatible with and is used in conjunction with a hierarchical file system, such as FAT or NTFS, col. 4, line 56-65)*;

examining the attributes of each file and determining whether a file is resident or non resident *(i.e. the disk can be scanned to find missing files, col. 4, line 66 to col. 5, line 11; a flag in the directory entry and in each data block is set to indicate that the file is no longer present, col. 10, lines 12-16)*;

backing up entire attributes of a file *(i.e. A second possible mode of operation is to back up files asynchronously (e.g. during idle time or at prespecified intervals). Again, a supervisory program monitors disk operations, <u>tracking those files that have been created or changed on the FAT file system</u>. Then, periodically or during idle time, the supervisory program takes appropriate action to copy, modify, or erase the data on the device embodying the file system, as indicated by the tracking information discussed above, col. 10, lines 57-65)* if it is determined

that the file is resident *(i.e. File allocation information can be dynamically maintained and can be reconstructed in cases of loss or damage by scanning the disk for blocks having identification and sequence numbers, col. 4, line 66 to col. 5, line 11)*; and

backing up attributes and data blocks belonging to the file *(i.e. A second possible mode of operation is to back up files asynchronously (e.g. during idle time or at prespecified intervals). Again, a supervisory program monitors disk operations, <u>tracking those files that have been created or changed on the FAT file system</u>. Then, periodically or during idle time, the supervisory program takes appropriate action to copy, modify, or erase the data on the device embodying the file system, as indicated by the tracking information discussed above, col. 10, lines 57-65)* if it is determined the file is not resident *(i.e. Only a small portion of each data file block is devoted to the information used to recreate the file and directory structures, col. 5, lines 12-25)*.

5. Claims 1-3, 6, 13-15, 18, 25, 27 are rejected under 35 U.S.C. 102(e) as being anticipated by Dunham et al. (US Patent No. 6,269,431).

Dunham anticipated independent claims 1, 13, 25 by the following:

As per claim 1, Dunham teaches a serverless backup system for backing up information on a network including one or more servers, comprising

a storage system *(See Figs. 1, 2)* for storing information to be backed up and restored *(i.e. The data storage subsystem has primary data storage, and the backup versions are stored in secondary data storage linked to the data storage subsystem for transfer of the backup versions from the secondary data storage to the data storage subsystem, col. 1, line 60 to col. 2, line 18)*, the storage system operable to:

receive the information *(i.e. The host computer 20 is operated by a user 23, and during typical operation the host computer reads and writes to primary storage 27 in the primary data storage subsystem 21. In order to recover from a failure causing a loss of data in the primary storage 27, a backup copy of data in the primary storage 27 is kept in secondary storage 29 of the secondary data storage subsystem 22, col. 5, lines 14-25)* from a plurality of workstations *(i.e. Host 31, 32, 33, Fig. 2)*; and

store the information *(i.e. The host computer 20 is operated by a user 23, and during typical operation the host computer reads and writes to primary storage 27 in the primary data storage subsystem 21. In order to recover from a failure causing a loss of data in the primary storage 27, a backup copy of data in the primary storage 27 is kept in secondary storage 29 of the secondary data storage subsystem 22, col. 5, lines 14-25)* received from the plurality of workstations *(i.e. The hosts 31, 32, 33, for example, are workstations of respective users 34, 35, 36, col. 8, lines 16-43)*; and

a backup storage system for backing up the information *(i.e. The data storage subsystem has primary data storage, and the backup versions are stored in secondary data storage linked to the data storage subsystem for transfer of the backup versions from the secondary data storage to the data storage subsystem, col. 1, line 60 to col. 2, line 18)*, the backup storage system coupled to the storage system and to one or more servers via network *(i.e. Control station server 76, 77, See Fig. 4)*;

wherein:

the information being backup is transferred using one or more data movers *(i.e. data mover 72, 73, 74, 75, See Fig. 4)* operable to transfer the information being backed up

directly *(i.e. The storage controller has at least one data port for linking the primary data storage and the secondary data storage to the host processor for transfer of data between the primary data storage and the secondary data storage and the host processor, col. 3, line 48 to col. 4, line 23)* from the storage system *(i.e. primary data storage, col. 1, line 60 to col. 2, line 18)* to the backup storage system *(i.e. the backup versions are stored in secondary data storage, col. 1, line 60 to col. 2, line 18)* without going through the one or more servers *(i.e. specified data in the primary storage 27 is copied to the secondary storage 29 when the primary data storage subsystem 21 receives a backup command from the host 20, col. 5, lines 26-44)*; and

the information being restored is transferred using one or more data movers *(i.e. data mover 72, 73, 74, 75, See Fig. 4)* operable to transfer the information being restored directly *(i.e. The storage controller has at least one data port for linking the primary data storage and the secondary data storage to the host processor for transfer of data between the primary data storage and the secondary data storage and the host processor, col. 3, line 48 to col. 4, line 23)* from the backup storage system *(i.e. the backup versions are stored in secondary data storage, col. 1, line 60 to col. 2, line 18)* to the storage system *(i.e. primary data storage, col. 1, line 60 to col. 2, line 18)* without going through the one or more servers *(i.e. The data storage subsystem has primary data storage, and the backup versions are stored in secondary data storage linked to the data storage subsystem for transfer of the backup versions from the secondary data storage to the data storage subsystem, col. 1, line 60 to col. 2, line 18).*

As per claim 13, Dunham teaches a serverless backup method for backing up information on a network including one or more servers, comprising:

providing a storage system *(See Figs. 1, 2)* for storing information to be backed up and restored *(i.e. The data storage subsystem has primary data storage, and the backup versions are stored in secondary data storage linked to the data storage subsystem for transfer of the backup versions from the secondary data storage to the data storage subsystem, col. 1, line 60 to col. 2, line 18)*, the storage system operable to:

receive the information from a plurality of workstation *(i.e. The host computer 20 is operated by a user 23, and during typical operation the host computer reads and writes to primary storage 27 in the primary data storage subsystem 21. In order to recover from a failure causing a loss of data in the primary storage 27, a backup copy of data in the primary storage 27 is kept in secondary storage 29 of the secondary data storage subsystem 22, col. 5, lines 14-25)*; and

store the information received from the plurality of workstations *(i.e. The host computer 20 is operated by a user 23, and during typical operation the host computer reads and writes to primary storage 27 in the primary data storage subsystem 21. In order to recover from a failure causing a loss of data in the primary storage 27, a backup copy of data in the primary storage 27 is kept in secondary storage 29 of the secondary data storage subsystem 22, col. 5, lines 14-25)*;

providing a backup storage system for backing up the information *(i.e. The data storage subsystem has primary data storage, and the backup versions are stored in secondary data storage linked to the data storage subsystem for transfer of the backup versions from the secondary data storage to the data storage subsystem, col. 1, line 60 to col. 2, line 18)*, the backup storage system coupled to the storage system and to one or more servers via a network *(i.e. Control station server 76, 77, See Fig. 4)*;

backing up the information by transferring the information using one or more data movers *(i.e. data mover 72, 73, 74, 75, See Fig. 4)* operable to transfer the information being backed up directly *(i.e. The storage controller has at least one data port for linking the primary data storage and the secondary data storage to the host processor for transfer of data between the primary data storage and the secondary data storage and the host processor, col. 3, line 48 to col. 4, line 23)* from the storage system to the backup storage system without going through the one or more servers *(i.e. specified data in the primary storage 27 is copied to the secondary storage 29 when the primary data storage subsystem 21 receives a backup command from the host 20, col. 5, lines 26-44)*; and

restoring information by transferring information using one or more data movers *(i.e. data mover 72, 73, 74, 75, See Fig. 4)* operable to transfer the information being restored directly *(i.e. The storage controller has at least one data port for linking the primary data storage and the secondary data storage to the host processor for transfer of data between the primary data storage and the secondary data storage and the host processor, col. 3, line 48 to col. 4, line 23)* from the backup storage system to the storage system without going through the one or more servers *(i.e. The data storage subsystem has primary data storage, and the backup versions are stored in secondary data storage linked to the data storage subsystem for transfer of the backup versions from the secondary data storage to the data storage subsystem, col. 1, line 60 to col. 2, line 18).*

As per claim 25, Dunham teaches a computer readable medium including code for performing a serverless backup method for backing up information on a network, the network

including a storage device for storing information to be backed up and restored *(i.e. The data storage subsystem has primary data storage, and the backup versions are stored in secondary data storage linked to the data storage subsystem for transfer of the backup versions from the secondary data storage to the data storage subsystem, col. 1, line 60 to col. 2, line 18)*, the storage system operable to receive the information form a plurality of workstations and store the information received from the plurality of workstations *(i.e. The host computer 20 is operated by a user 23, and during typical operation the host computer reads and writes to primary storage 27 in the primary data storage subsystem 21. In order to recover from a failure causing a loss of data in the primary storage 27, a backup copy of data in the primary storage 27 is kept in secondary storage 29 of the secondary data storage subsystem 22, col. 5, lines 14-25)*, the network further including a backup storage system for backing up the information, the backup storage system coupled to the storage system and to one or more servers via the network, the code comprising:

code for backing up the information by transferring the information using one or more data movers *(i.e. data mover 72, 73, 74, 75, See Fig. 4)* operable to transfer the information being backed up directly*(i.e. The storage controller has at least one data port for linking the primary data storage and the secondary data storage to the host processor for transfer of data between the primary data storage and the secondary data storage and the host processor, col. 3, line 48 to col. 4, line 23)* from the storage system to the backup storage system without going through the one or more servers *(i.e. specified data in the primary storage 27 is copied to the secondary storage 29 when the primary data storage subsystem 21 receives a backup command from the host 20, col. 5, lines 26-44)*; and

code for restoring the information by transferring the information using one or more data movers *(i.e. data mover 72, 73, 74, 75, See Fig. 4)* operable to transfer the information being restored directly *(i.e. The storage controller has at least one data port for linking the primary data storage and the secondary data storage to the host processor for transfer of data between the primary data storage and the secondary data storage and the host processor, col. 3, line 48 to col. 4, line 23)* from the backup storage system to the storage system without going through the one or more servers *(i.e. The data storage subsystem has primary data storage, and the backup versions are stored in secondary data storage linked to the data storage subsystem for transfer of the backup versions from the secondary data storage to the data storage subsystem, col. 1, line 60 to col. 2, line 18).*

As to claims 2, 14, Dunham teaches the backup storage system comprises a tape storage system *(i.e. the primary data storage subsystem 21, for example, is a cached disk data storage subsystem including a random access cache memory and magnetic disk data storage. As further described below with reference to FIG. 4, the secondary data storage subsystem 22, for example, includes a tape library unit containing a multiplicity of magnetic tape cassettes providing the secondary storage 29, col. 7, line 55 to col. 8, line 5).*

As to claims 3, 15, Dunham teaches the storage system comprises a disk storage system *(i.e. the primary data storage subsystem 21, for example, is a cached disk data storage subsystem including a random access cache memory and magnetic disk data storage. As further described below with reference to FIG. 4, the secondary data storage subsystem 22, for example,*

includes a tape library unit containing a multiplicity of magnetic tape cassettes providing the secondary storage 29, col. 7, line 55 to col. 8, line 5).

As to claim 6, 18, 27, Dunham teaches prior to transferring information directly form the storage system to the backup storage system, a snapshot of the storage system is taken *(i.e. Preferably, the primary directory 26 is constructed in such a way that the host can continue to access the primary storage 27 concurrently with the copying process. For example, in response to the backup command from the host 20, the primary data storage subsystem creates an "instant snapshot copy" of the specified physical storage unit, and this instant snapshot copy is protected from modification by the host 20 while the instant snapshot copy is being written to the secondary storage 29. There are a number of ways that such an instant snapshot copy can be created, depending on the way that the primary directory is organized, col. 5, line 57 to col. 6, line 6).*

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any

evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

7. Claims 4, 5, 16, 17, 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dunham et al. (US Patent No. 6,269,431), in view of Tamura (US Patent No. 6,728,848).

As to claims 4, 16, Dunham does not specifically teach the backup storage system comprises a storage area network.

Tamura teaches the backup storage system comprises a storage area network *(i.e. The storage system is coupled with the plurality of backup systems via a storage area network (SAN), col. 2, lines 25-35)*.

It would have been obvious to one of ordinary skill of the art having the teaching of Dunham and Tamura at the time the invention was made to modify the system of Dunham to include the limitations as taught by Tamura. One of ordinary skill in the art would be motivated to make this combination in order to back-up the information indicated in the E-copy command to the back-up device in view of Tamura (Abstract), as doing so would give the added benefit of providing an improved backup technique which further decentralizes the back-up of a storage system on a SAN to, for example, the storage system itself as taught by Tamura (col. 2, lines 7-10).

As to claims 5, 17, 26, Dunham teaches the system as recited in Claim 1, but does not specifically teach wherein the information is transferred between the backup storage system and the storage system using Extended Copy command.

Tamura teaches the information is transferred between the backup storage system and the storage system using Extended Copy command *(i.e. E-copy command, col. 2, lines 13-24).*

It would have been obvious to one of ordinary skill of the art having the teaching of Dunham and Tamura at the time the invention was made to modify the system of Dunham to include the limitations as taught by Tamura. One of ordinary skill in the art would be motivated to make this combination in order to back-up the information indicated in the E-copy command to the back-up device in view of Tamura (Abstract), as doing so would give the added benefit of providing an improved backup technique which further decentralizes the back-up of a storage system on a SAN to, for example, the storage system itself as taught by Tamura (col. 2, lines 7-10).

8. Claims 7, 19, 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dunham et al. (US Patent No. 6,269,431), in view of Clifton et al. (US Patent No. 6,081,875).

As to claims 7, 19, 28, Dunham does not specifically teach a period of write inactivity to the storage system is waited for prior to taking the snapshot.

Clifton teaches a period of write inactivity to the storage system is waited for prior to taking the snapshot *(i.e. such time as they are needed to construct the snapshot database image to be stored to BSU 150, col. 3, line 61 to col. 4, line 13).*

It would have been obvious to one of ordinary skill of the art having the teaching of Dunham and Clifton at the time the invention was made to modify the system of Dunham to include the limitations as taught by Clifton. One of ordinary skill in the art would be motivated to make this combination in order to construct the snapshot database image in view of Clifton (col. 3, line 61 to col. 4, line 13), as doing so would give the added benefit of allowing users unrestricted access to the system during the backup process while creating a snapshot backup image on tape that does not require reconstruction as taught by Clifton (col. 2, lines 17-21).

9. Claims 8, 9, 20, 21, 29, 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dunham et al. (US Patent No. 6,269,431), in view of Clifton et al. (US Patent No. 6,081,875), and further in view of Gold et al. (US Patent No. 6,785,786).

As to claims 8, 20, 29, Dunham, Clifton do not specifically teach the period of write inactivity is a predefined period of time.

Gold teaches the period of write inactivity is a predefined period of time *(i.e. if the time is set to 5 seconds, col. 5, lines 55-67)*.

It would have been obvious to one of ordinary skill of the art having the teaching of Dunham, Clifton, and Gold at the time the invention was made to modify the system of Dunham, Clifton to include the limitations as taught by Gold. One of ordinary skill in the art would be motivated to make this combination in order to determine when a file is safe to backup in view of Gold (col. 5, lines 54-67), as doing so would give the added benefit of having a data restore operation can be enacted using data stored in primary storage, without needing to find and install any particular backup tape (col. 2, lines 9-14) as taught by Gold.

As to claims 9, 21, 30, Dunham, Clifton, Gold do not expressly teach the predefined period of time is three seconds.

However, Gold teaches *"if the time is set to 5 seconds" (col. 5, lines 54-67).*

It would have been obvious to one ordinary skill of the art having the teaching of Dunham, Clifton, and Gold at the time the invention was made to set the predefined period of time of Gold to three seconds in order to determine when a file is safe to backup as taught by Gold (col. 5, lines 55-67), as doing so would give the added benefit of a data restore operation can be enacted using data stored in primary storage, without needing to find and install any particular backup tape (col. 2, lines 9-14) as taught by Gold.

10. Claims 8, 9, 20, 21, 29, 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dunham et al. (US Patent No. 6,269,431), in view of Clifton et al. (US Patent No. 6,081,875), and further in view of Blam et al. (US Patent No. 6,738,923).

As to claims 10, 22, 31, Dunham, Clifton do not explicitly teach if the period of write inactivity does not occur by time a timeout period has expired, the transfer fails.

However, Blam teaches a timeout period *(col. 4, line 65 to col. 5, line 27).*

It would have been obvious to one of ordinary skill of the art having the teaching of Dunham, Clifton, and Blam at the time the invention was made to modify the system of Dunham, Clifton to include the limitations as taught by Blam. One of ordinary skill in the art would be motivated to make this combination in order to access and boot from the next backup server in the network (col. 5, lines 15-27) in view of Blam, as doing so would give the added

benefit of adjusting time-outs and failover intervals according to the requirements of different systems (col. 1, line 65 to col. 2, line 3) as taught by Blam.

As to claims 11, 23, 32, Blam teaches the timeout period is a predefined period of time (i.e. *a method of adjusting failover intervals, col. 4, line 65 to col. 5, line 27).*

As to claims 12, 24, 33, Dunham, Clifton, Blam do not specifically teach the predefined period of time is 80 seconds.

However, Blam teaches *"a method of adjusting failover intervals" (col. 5, lines 59-67).*

It would have been obvious to one ordinary skill of the art having the teaching of Blam at the time the invention was made to use the method of Blame to adjust the predefined period of time is 80 seconds in order to access and boot from the next backup server in the network as taught by Blam (col. 5, lines 15-27), as doing so would give the added benefit of adjusting time-outs and failover intervals according to the requirements of different systems (col. 1, line 65 to col. 2, line 3) as taught by Blam.

Response to Arguments

11. Applicant's arguments regarding claim 34 filed 12/10/2007 have been fully considered but they are not persuasive for the following reasons:

(a). Spilo teaches determining whether a file is resident or non-resident.

Regarding Applicant's argument with respect to "Spilo does not teach 'determining whether a file is resident or non resident' as recited in Claim 34", the examiner notes that "claims

must be interpreted as broadly as their terms reasonably allow" (**In re Zletz**, 893 F.2d 319, 321, 13 USPQ2d 1320, 1322 (Fed. Cir. 1989); and, "the 'ordinary meaning' of a claim term is its meaning to the ordinary artisan after reading the entire patent." (**Phillips v. AWH Corp.,** 415 F.3d 1303, 1321, 1332 (Fed. Cir. 2005). Accordingly, since there is no specific definition of the term "resident, non resident" in the instant specification, and the claim language merely states "a file is resident or non resident", thereby, giving the broadest and most reasonable interpretation, the Examiner finds the ordinary meaning of the term "resident" is best found in dictionary. The Examiner notes that the definition most suitable for "resident" is "living in particular place" (see attached search note: <wordnet.princeton.edu/perl/webwn>); thus, Spilo discloses "the disk can be scanned to find missing files" as to determine whether the files belong to the disk read on "determining whether a file is resident or non-resident". It is noted that ccording to the <wordnet.princeton.edu/perl/webwn>, "missing" means "not able to be found", therefore, "missing file" equates to "non resident file". It is further noted that, Spilo also discloses a flag as an indication of residency of a file, col. 10, lines 12-16 *(i.e. a flag in the directory entry and in each data block is set to indicate that the file is no longer present, col. 10, lines 12-16).* Therefore, the terms "no longer present" or "present"of Spilo, hence, equates to the term "resident" or "non resident" of the claimed invention, respectively.

<u>(b). Spilo teaches backing up entire attributes of a file if it is determined that the file is resident.</u>

Regarding Applicant's argument with respect to "Spilo does not teach 'backing up entire attributes of a file if it is determined that the file is resident', as recited in Claim 34", the

examiner notes that Spilo teaches the step of backing up files in col. 10, lines 42-65 *(i.e. One such possibility is to use the file system for real-time backups; A second possible mode of operation is to back up files asynchronously).*

According to the teachings of Spilo, in order to back up files from the disk drive 29 to the disk drive 18 *(i.e. If a disk file is written, modified, or deleted on the FAT file system (such as on the disk drive 20, FIG. 1), the supervisory program would take appropriate action to copy, modify, or erase the data on a device embodying the file system of the invention (such as the disk drive 18), col. 10, lines 42-56, Spilo),* a supervisory program monitors disk operation, tracking those files that have been created or changed on the FAT file system (the disk drive 20), then the supervisory program takes appropriate action to copy, modify or erase the data on the device embodying the file system (the disk drive 18) *(i.e. A second possible mode of operation is to back up files asynchronously (e.g. during idle time or at prespecified intervals). Again, a supervisory program monitors disk operations, tracking those files that have been created or changed on the FAT file system. Then, periodically or during idle time, the supervisory program takes appropriate action to copy, modify, or erase the data on the device embodying the file system, as indicated by the tracking information discussed above, col. 10, lines 57-65, Spilo).*

According to the step of tracking those files of Spilo, if the file has been modify, i.e. this file is **present in the disk drive 18**, the supervisory program takes appropriate action to modify the data on the disk drive 18. This step of Spilo equal to the claimed limitation "Backing up entire attributes of a file if it is determined that the file is resident".

The entire attributes of the claimed limitation equates to the proper file sequence number *(i.e. When appending to or modifying a file, the same file identification number 62 should be*

used on the added or changed blocks as is used by the existing file; the proper file sequence numbers 64 should be determined and allocated as necessary. When truncating a file, the file sequence numbers 64 for discarded data blocks should be obliterated, so the discarded blocks are not re-attached when a damage repair operation is performed, as will be discussed below, col. 10, lines 27-37; Each allocation block within a single file (as in the illustrated file 50) also has a unique sequence number 64. For example, file 50 is four blocks in length, so the number 1 will be stored as the sequence number within the signature area 60 of the first block 52, the number 2 will be stored within the signature area 60 of the second block 54, the number 3 will be stored within the third block 56, and the number 4 will be stored within the fourth block 58, col. 8, lines 24-33). It should be noted that each block within a single file of Spilo has a sequence number, and then the proper file sequence number of that file contains a plurality of sequence numbers. Therefore, the entire attributes of the file of the claimed invention should be equated to the proper file sequence number of Spilo. When a file is modified, the proper file sequence number would be changed *(i.e. When appending to or modifying a file, the same file identification number 62 should be used on the added or changed blocks as is used by the existing file; the proper file sequence numbers 64 should be determined and allocated as necessary, col. 10, lines 27-37),* thus, the step of modify the data on the disk drive 18 as mentioned above implies the step of modifying the proper file sequence. This step corresponds to the step of "backing up entire attributes" of the claimed limitation.

(c). Spilo teaches backing up attributes and data blocks belonging to the file if it is determined that the file is non-resident.

Regarding Applicant's argument with respect to "Spilo does not teach 'backing up entire attributes and data blocks belonging to the file if it is determined that the file is non-resident', as recited in Claim 34", the Applicants' argument is not persuasive under the same rationale given above to arguments (a) and (b).

According to the step of tracking those files of Spilo, if the file has been created, i.e. this file is **not present in the disk drive 18**, the supervisory program takes appropriate action to copy data to the disk drive 18. This step of Spilo, hence, corresponds to the claimed limitation "backing up attributes and data blocks belonging to the file if it is determined that the file is non-resident".

Therefore, the claim language as presented is still read on by the Spilo reference at the cited paragraph in the claim rejections. Arguments as raised are moot since all claim limitations relevant to this issue have been addressed accordingly.

12. With respect to claims 1-33, Applicants have amended the independent claim 1, 13, 25 to recite "using one or more data movers operable to transfer the information being backed up/restored"; however, upon further search and consideration, a new ground(s) of rejection is made in view of newly found prior art.

Conclusion

13. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Miranda Le whose telephone number is (571) 272-4112. The examiner can normally be reached on Monday through Friday from 8:30 AM to 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John R. Cottingham, can be reached on (571) 272-7079. The fax number to this Art Unit is (571)-273-8300.

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (571) 272-2100..

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Miranda Le/

Primary Examiner, Art Unit 2167

April 06, 2008